CLAIMS

What is clamed is:

1. A method for generating a unique, one way, compact mnemonic credential for identifying and separately authenticating a voter while maintaining voter privacy comprising:

defining a database for identification of voters, wherein said data base comprises registration data for each voter;

defining a collision index corresponding to each voter in said database, wherein the collision index is a number unknown a priori;

defining an authentication record for each voter, assigning a subset from a selected set of characters to each voter in the database;

providing a computer means for calculating said collision index which is used to select a different authentication record, such that each voter authentication record is unique within a given length;

creating thus a one way mapping of a higher dimensional argument space onto a lower dimensional space without collisions such that the mapping cannot be inverted.

2. A method for generating a unique, one-way, compact credential for identifying and separately authenticating a voter while maintaining voter privacy as in claim 1 further comprising:

applying the collision index as part of an argument of a hash function used to select a different authentication record, such that each voter authentication record is unique within a given length; wherein the hash function creates thus a one way mapping of a higher dimensional argument space onto a lower dimensional space without collisions and so that the hash function cannot be inverted.

3. A method for generating a unique, one way, compact mnemonic credential for identifying and separately authenticating a voter according to claim 1 further comprising:

translating the credential into a mnemonic string according to a language rule while preserving credential uniqueness in that language.

4. A method for generating a unique, one-way compact mnemonic credential for identifying and separately authenticating a voter while maintaining voter privacy as in claim 1 further comprising:
providing a verification key of sufficient length to enable a verifier to authenticate information encoded in the credential while enabling the credential to be made secure against attacks.

5. A method for generating a unique, one way compact c credential for identifying and separately authenticating a voter while maintaining voter privacy as in claim 4 comprising:
providing a local feedback loop, responsive to the collision index for ensuring information encoded in the credential shall be reliably discovered only by a verifier that has the correct verification key

6. A method for generating a unique, one way, compact credential for identifying and separately authenticating a voter over a communication channel while maintaining voter privacy comprising:

defining a database for identification of voters, wherein said data base comprises registration

data for each voter;

defining a collision index corresponding to each voter in said database, wherein the collision index is a number unknown a priori;

defining an authentication record for each voter by assigning a subset from a selected set of characters to each voter in the database;

calculating a one-way mapping without collisions from said collision index such that a different authentication record is selected wherein each voter authentication record is unique within a given length; and wherein the voter authentication record provides a credential unique to each voter;

translating the credential into a data packet matched to a specific type of communication channel for transporting said credential from a source to a destination along said communication channel;

7.A method for providing a unique, one way voter credential comprising:
providing a voter database comprising voter registration data for each voter;

providing a unique voter credential for each voter;

providing a voter index corresponding to each voter in the voter data base;

mapping the unique voter credential to the voter index for each voter to create a voter data table;

using a one way function to map without collisions in the result space, each record in the voter data table, to another set of data as a result space, such that the argument space can have collisions and can be larger than the result space and knowledge of the result does not provide knowledge of the voter data.

8. A method for automatically generating unique voter credentials at a registrar service that are one-way and short comprising:

providing a plurality of voter registration files containing private voter data;

assigning an initial collision index and a header data to each voter file;

hashing the voter file with the initial collision index and the header data into a canonical form;

folding the canonical form and producing a result with reduced length;

calculating a modulo division of the result to further reduce its length and thus produce a pre-credential;

encoding the pre-credential into a desired mnemonic form for a credential such that each credential is unique among all previously calculated credentials for the voter registration files and wherein said credential may be used to identify and/or authenticate the voter to a selected third-party and/or to the registration service without loss of voter privacy.

9. A method according to claim 8 further comprising;

verifying whether the encoded credential is unique among all previously calculated credentials for the voter registration files; and

if the credential is not unique, assigning a new collision index and reiterate the method by hashing the voter file with the new collision index, until the credential is unique;

10. A method according to claim 8 further comprising translating the credential into a mnemonic string according to a language rule while preserving credential uniqueness.